(12) **UK Patent Application** (19) **GB** (11) **2 315 804** (13) **A**

(21) Application No 9615898.5

(22) Date of Filing 29.07.1996

(71) Applicant(s)
Christopher James Hunter
6 St Margarets Rd, MAIDENHEAD, Berks, SL6 5DZ,
United Kingdom

(72) Inventor(s)
Christopher James Hunter

(74) Agent and/or Address for Service
Christopher James Hunter
6 St Margarets Rd, MAIDENHEAD, Berks, SL6 5DZ,
United Kingdom

(51) INT CL^6
E05B 49/00

(52) UK CL (Edition P)
E2A ALV A401 A420

(56) Documents Cited
GB 2260563 A   GB 2259737 A   GB 2188762 A
WO 86/01360 A1   WO 86/00108 A1   WO 80/02711 A1
WO 80/00091 A1

(58) Field of Search
UK CL (Edition O) E2A AEE ALV
INT CL^6 E05B 49/00

(54) **Programmable key and lock**

(57) A programmable security lock which is programmed with a security code which controls the opening of a catch thereof, said lock comprising an electronic key part (A) which is programmed with a security code which corresponds to that of a lock part (B), in which the key part (A) is capable of opening the catch when it has been coupled to said lock part (B) and when comparison means has confirmed agreement of the security code.

(A)

Figure 2

(B)

GB 2 315 804 A

(A)

(B)

(C)

(D)

Figure 1

(A)

(B)
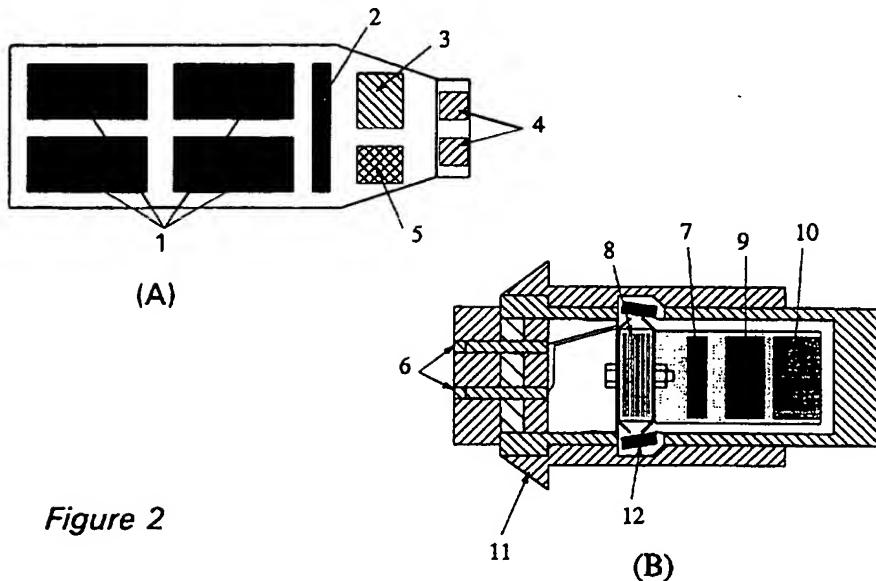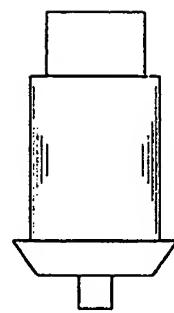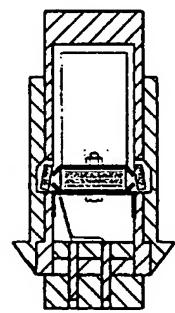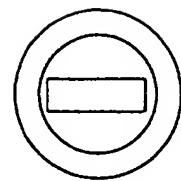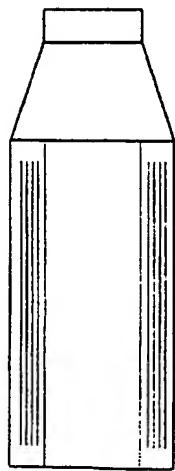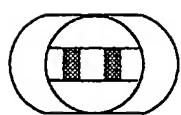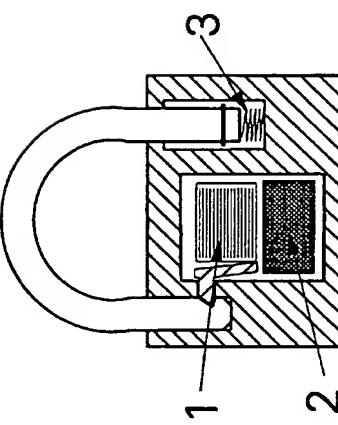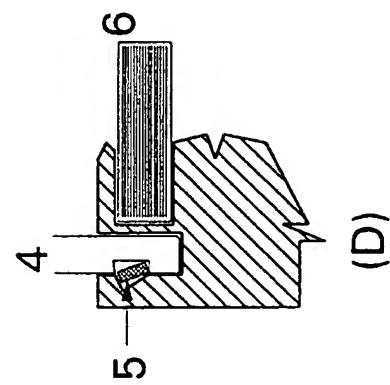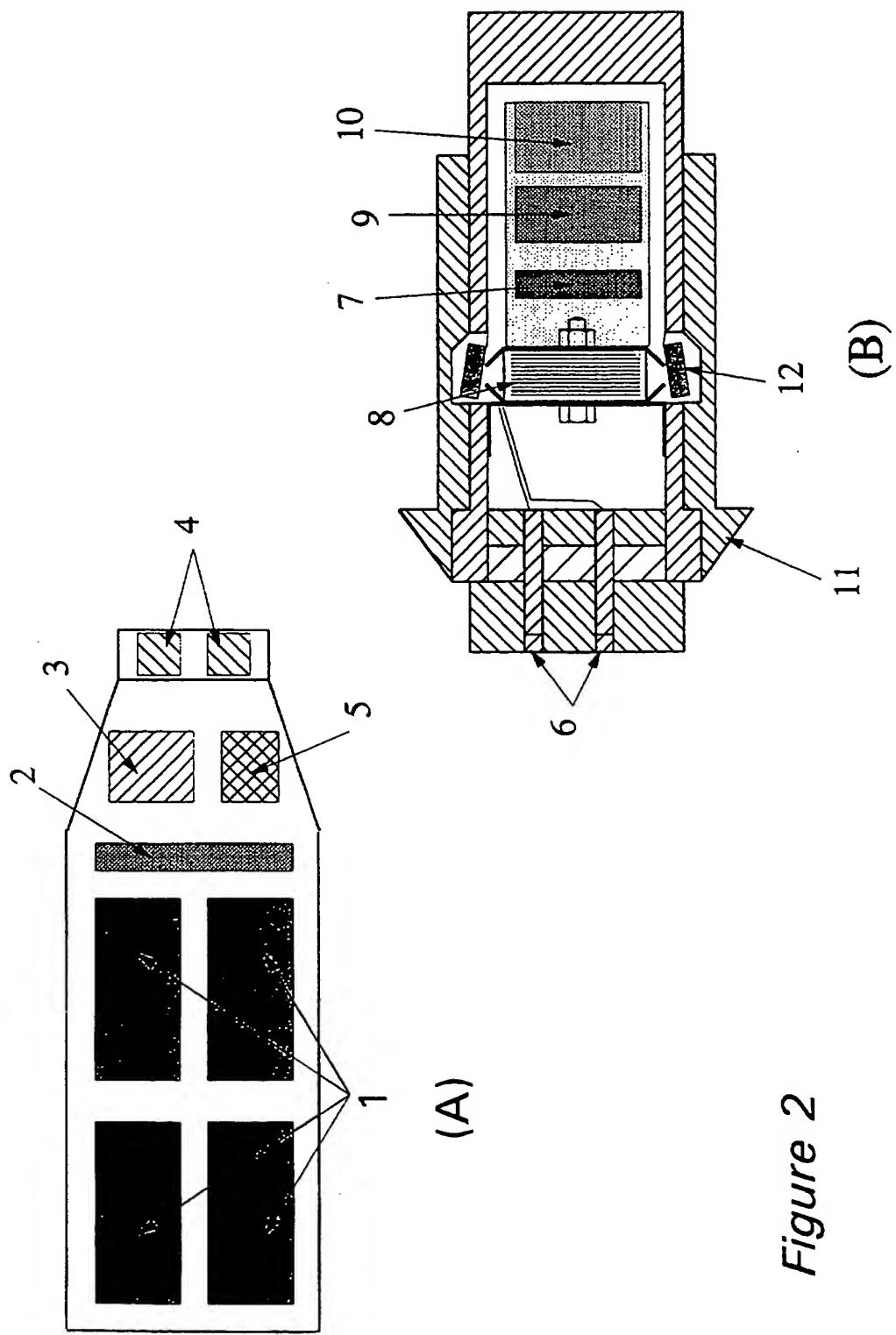
Figure 2

Typical sequnce of key and lock events

Figure 3

Programming Means

Key part 1

Key Part 2

Key Part 3

Zone 1

Zone 2

Zone 3

Lock Part 1

Lock Part 2

Lock Part 3
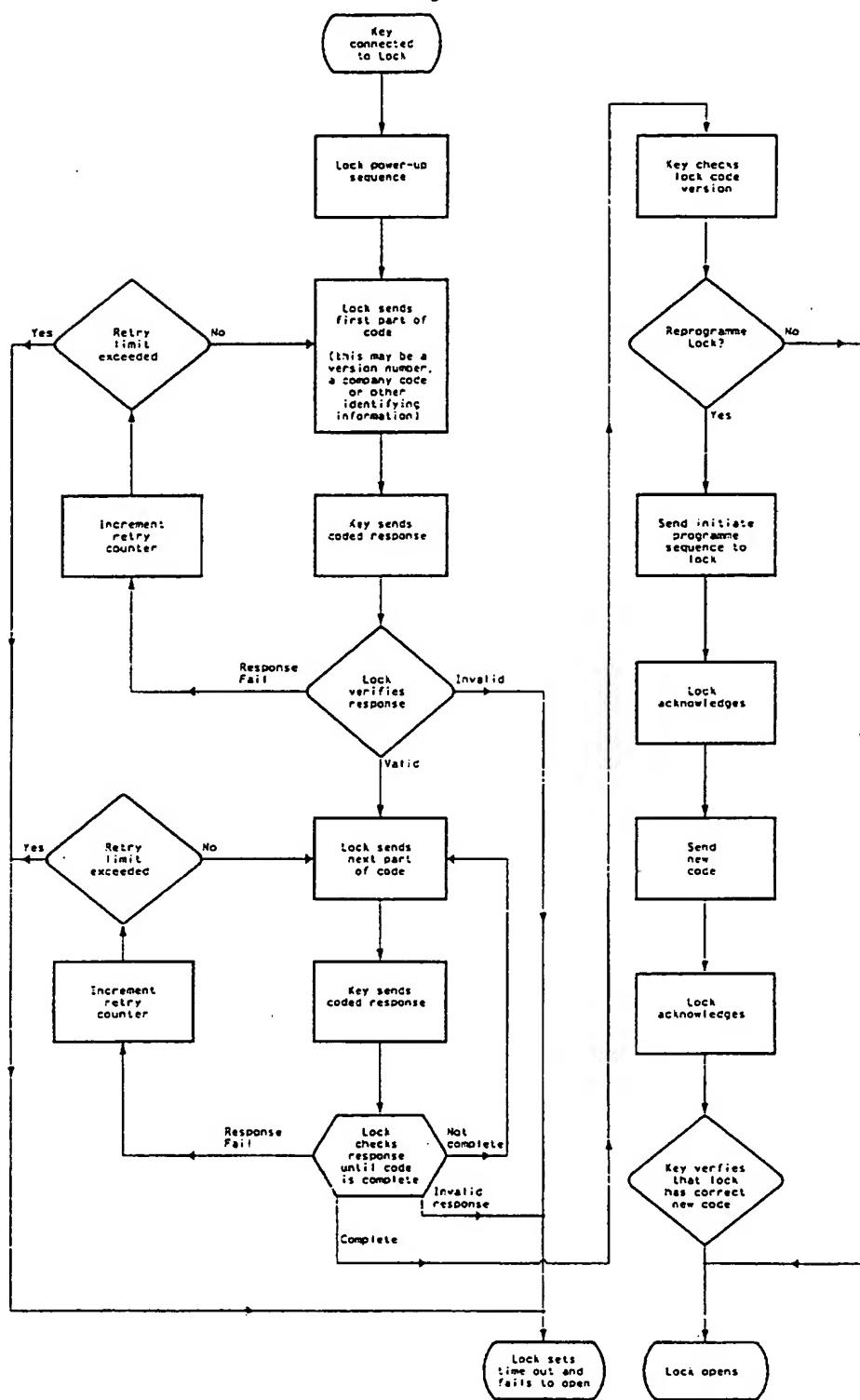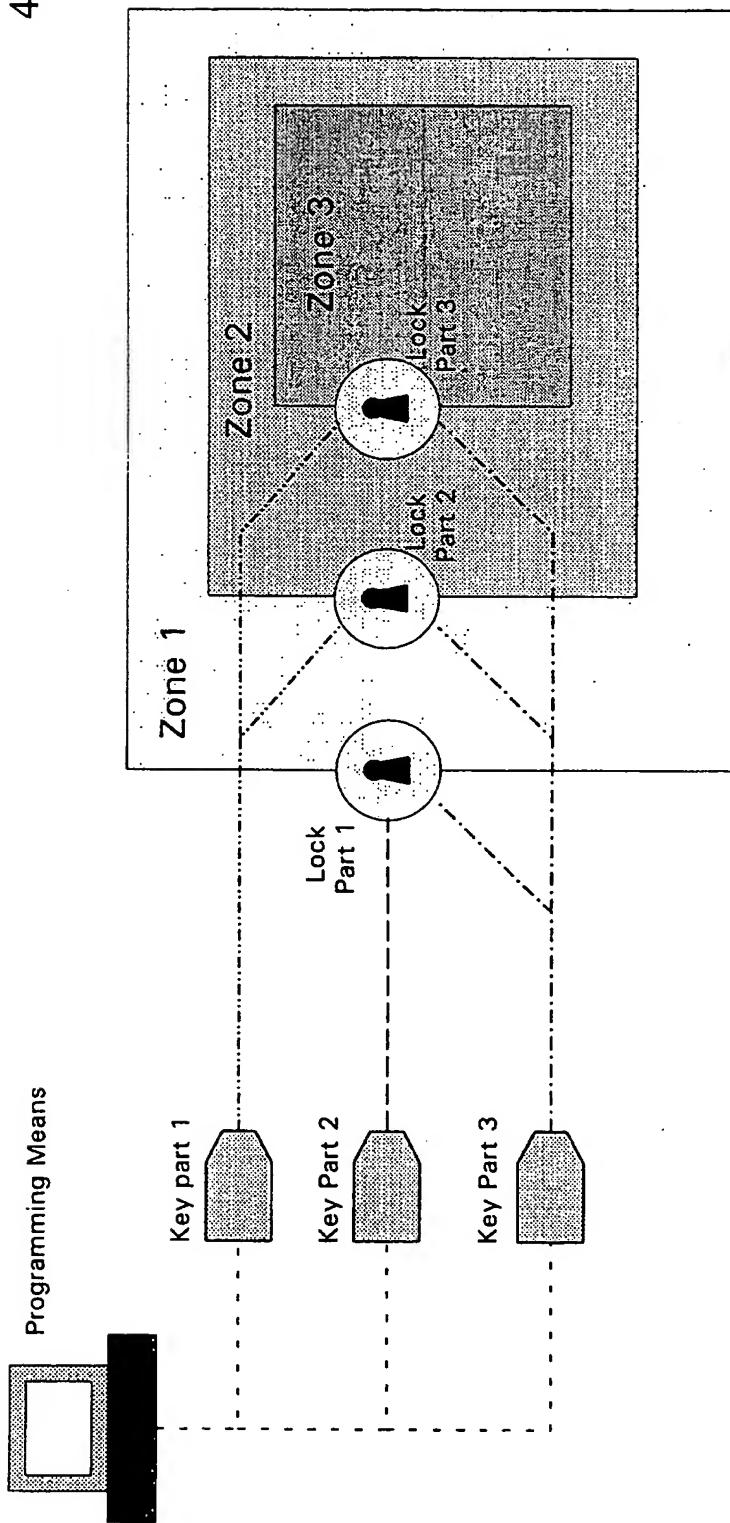
Figure 4

This invention relates to a programmable security lock. It relates particularly to a security lock and key system which can be programmed and reprogrammed as necessary with a security code to ensure that a given standard of security is maintained.

Background

Electronic locks and keys are well known, particularly as applied to vehicle locks. Such electronic locks require a power source to actuate the lock, after the key has been validated, to enable the opening of the lock. This is easily achieved in a vehicle since the vehicle battery is more than capable of powering a locking system. In a building provision of power to an electronic lock may be more difficult to achieve as additional wiring would be required and a power failure would also lead to failure of the lock. In other applications such as padlocks provision of power from an external source is very difficult. The use of batteries in the lock requires them to be replaced or recharged and this may not be convenient due to the location of the lock.

US patent no. 4,594,637 describes a digital electronic lock system in which the lock is actuated by a power supply contained in a small portable housing. This housing also contains a keypad or other device to provide a code to cause the lock to open. GB patent 2,184,159 describes an electronic padlock which

1

is powered by inductive coupling to a key. This device is also reprogrammable.

Such reprogrammable locks are also well known. Clearly security is much improved if the code in a lock can be altered periodically. The ability to reprogramme the lock gives the added benefit that if the keys are lost or stolen the lock does not need to be replaced, merely reprogrammed. This reprogramming is analogous to changing the combination of a combination lock, such locks are used in all manner of applications from briefcases to safes. Reprogramming an individual lock is not a significant problem but reprogramming a number of locks may become time consuming task, especially if they are geographically distributed over a wide area.

Very well known are locks which are opened by a plurality of keys, it being normal to have several keys for one lock, and keys which open a plurality of locks. The most common situation with the latter application is to simply produce a number of identical locks which can then be opened by the same key. The problem with this situation is that if a lock is replicated anyone with the appropriate key can open the lock and control of access is lost. Similarly if a key is stolen all the locks must be changed to ensure security. With any lock, having only one key can present problems as can having several keys. If only one key exists and this is lost then the lock cannot be opened. If several keys exist then security may be compromised and if the lock is used for safety reasons, to lock off an electricity supply for example, then an unsafe situation may be brought about. A further problem is that every lock and key arrangement requires a key, given the increasing use of locks for

security and safety purposes, this inevitably leads to a profusion of keys which need to be managed and controlled.

Description

The present invention provides some solutions to the problems described above in a number of ways. All the previously described devices place the emphasis on the lock as the means of providing access control. Clearly the lock is the element of the arrangement which provides the physical barrier but, in general, it is the key which is transportable and the key which needs to be managed to maintain safe, secure access control. The present invention removes the dependence of the key on the lock and allows the key to be controlled.

Traditionally a lock is purchased with keys and in general further keys may be cut, with the exception of specialist locks for which only one key exists. The present invention is a key which is reprogrammable and which can reprogramme the lock automatically or on the instruction of the operator, or after verification which may or may not require the intervention of the operator. The key contains a programmable or re-configurable device and some form of memory or means of storing the configuration, if this is not integral to the programmable or re-configurable device, as well as a power supply. Similarly the lock would contain a memory or means of storing the configuration.

Throughout this description the term reprogrammable is used to indicate an electronic device which can be reprogrammed. Such an electronic lock and key system would work be means of exchanging an electronic code between the lock and key. It is also envisaged that the present invention could be achieved by mechanical means by having a key which can be re-configured. Such a mechanically re-configurable key could transfer a new configuration to a re-configurable lock.

In normal operation the key would be inserted into, attached to, or in some other way connected to the lock and the lock would verify that the key is programmed or configured to open the lock. During the verification process the key would determine the current status of the code or configuration being used by the lock. If the key contains a newer code this would be programmed into the lock, after the lock has verified the key. Following this reprogramming the lock release mechanism would actuate allowing the lock to be opened. If the lock does not need reprogramming then the release mechanism would actuate after verification.

To enable the key to open several locks the key may contain a number of memory locations or configuration stores. The locks would all contain unique codes (or configurations) and would therefore not be copies of each other, but all could be opened by a correctly programmed or configured key.

All keys are a means of providing power to the lock to actuate the release of the locking mechanism. The act of inserting a conventional key into a

4

mechanical lock achieves this. In the present invention the preferred system is for electro-mechanical actuation of the lock release mechanism but other methods such as mechanical, magnetic, inductive, and thermal may be used. For the electro-mechanical application the key may have a rechargeable power source integral to the key but other options such as a separate power pack, power from mains or from a vehicle battery, alternator or dynamo, or separate generator set have been considered. The power source would actuate the lock release through the key thus eliminating the need for a power source in the lock.

The code used for the validation of the key by the lock may contain many levels of coded data. Information about the owner of the key, its programme version and data versions may all be encoded. Many locks, especially padlocks are used in safety related applications. In these circumstances it is desirable to give people restricted access to certain areas at particular times or in particular circumstances. By encoding zone information into the key and lock it is possible to control which groups of locks a key will open. All key holders may be granted access to the outer zone (zone 1 for example); a zone 1 key may also allow access to areas where there is no risk. Access to the next zone (zone 2 for example) may be restricted to certain personnel. A zone 2 key will allow access to zones one and two. This arrangement can be repeated any number of times providing a series of nested zones. An alternative arrangement is where access is restricted unless two or more people are present. In this case the zones may be exclusive, ie. a zone 1 key only opens zone one locks, a zone 2 key only zone 2 locks. This would ensure

5

that to access zone 2, if zone 2 was inside a zone 1 perimeter, a zone one key and a zone 2 key would be needed.

A further safety related application is the situation where it is necessary to know exactly how many personnel are in a restricted area. By installing a gate, door or turnstile and issuing personnel with a key, the lock could count the number of personnel entering and leaving. The lock could also record which keys opened it and therefore the identification of the personnel could be determined. The lock could be provided with a display to indicate the number and/or identification of the personnel within the restricted area.

Another safety related application is to connect the lock to an electrical interlock. At present mechanical key switches are used for this, but the present invention allows this to be achieved entirely electronically. The lock (whether or not including some mechanical element) may also be connected to a central control system, computer network, telemetry system, or other arrangement so that the lock condition, open/closed, and any recorded parameters may be ascertained remotely. This facility and/or the interlock arrangement may be used to disable warning alarms on plant, equipment, property boundaries or buildings so that warnings or alarms are not caused by legitimate entry or unlocking.

It is necessary to provide a means for programming and reprogramming (or configuring/re-configuring) the key. This may be achieved by means provided as part of the key or as a separate programmer. For an integral programmer a

6

key pad or other form of input device may be included as part of the key. In the case of a separate programmer the programmer may be a stand-alone device or as a device to be used in conjunction with a computer. Such a programmer may also act as a recharger for the key, if the key contains a rechargeable power source. The programmer, recharger or combined unit may be powered by mains electricity, the electric supply from a vehicle, a power source derived from a computer or other suitable source.

The reprogramming and/or recharging unit described above may also act as a key safe so that if the key is removed without proper validation (by password, application of another key or other means) then the key would be rendered invalid. The reprogramming and/or recharging unit may hold one or several keys at a time. This unit could be installed on a desk, wall, in a vehicle or be portable. The reprogrammer, whether a stand-alone unit or a computer peripheral, could also be used to store the details of the locks and keys currently in use. This would allow any number of keys to be programmed to suit the locks and allow keys to be set up to reprogramme the locks as and when required. The information held by the reprogrammer would need to be encrypted to protect against malicious use. The reprogrammer could also act as a system to store details about key and lock usage, this being down-loaded from the key.

The key may contain a display to allow the operator to monitor information about the lock, or for trouble-shooting purposes if the lock fails to open when expected. A key with a display could be used to display information

stored by the lock such as when the lock was last operated, which key last operated it, how often the lock has been opened or closed, the zonal information for the lock, or any other parameter recorded by the lock. Such information may also be down loaded into the key, or into a portable computer, for later processing, storage or printing.

A description of the drawings will now be given. The drawings set out only one application of the present invention and in no way are intended to restrict the application of this invention to the drawings and the following description.

Figure 1 shows general arrangements of the key and lock barrel along with two padlock applications. Figure 1A shows the key in front and side elevation, and plan view, figure 1B shows an example of a lock barrel in sectional elevation, front elevation and plan. In figure 1A the key is shown with a slot which can locate on to the raised face of the lock and provide a mechanical as well as an electrical connection. The mechanical connection provides a means of rotating the lock barrel (fig 1B) after the release pins have been withdrawn. The barrel could be built into a handle or lock body sized to suit standard fittings. Figure 1C shows a sectional view of the invention in a padlock, here solenoid (1) would retract after validation of the key by the electronics package (2). Spring (3) would open the hasp after retraction of the solenoid thus removing the need for any mechanical interaction between the key and lock, or on the part of the operator. Figure 1D shows a part section of an alternative arrangement where the pawl (5) holding the padlock in the closed

8

position is mounted on the hasp (4) and held in the locked position by a spring between the pawl and hasp. To open the lock, electromagnet (6) would be energized after validation of the key. Provided that the hasp and pawl are magnetically permeable the pawl would be pulled in by the magnetic flux from the electromagnet.

Figure 2 shows a block diagram of the key and lock. Referring to figure 2A, which shows the key, the battery pack (1) is connected to the ancillary electronics package (2) which provides voltage regulation, a clock signal for the microcontroller, recharging control, and power and signal supply to the lock. This package also powers the microcontroller (3). The microcontroller provides signals to, and decodes signals from the lock via the ancillary electronics. After appropriate validation for the key by the lock the microcontroller would reprogramme the lock if necessary. Additional memory storage may be provided (4). Either the memory in the microcontroller or the additional memory will be of the EEPROM type (or other non-volatile type) Power and signals are transferred to the lock via one, or a plurality of, connectors (5), two being shown in the figure.

The connectors (5) in figure 2A mate with the lock connectors (6) in figure 2B. Via these connectors power is provided to the lock electronics. These consist of ancillary electronics (7), a microcontroller (8) and additional memory (9) if required. Either the memory in the microcontroller or the additional memory will be of the EEPROM type (or other non-volatile type) to allow reprogramming by the key. On receiving power from the key the

microcontroller would execute a programme and after an exchange of codes with the key would validate the key. If the key is validated the solenoid (10) would retract the locking pins (12) allowing the lock to be opened. The lock barrel in figure 2B is shown in a bezel (11) for mounting in a door or lock body.

In addition to the basic system described above the key and lock could contain a number of additional features. The key could contain a time limiting device such that it would fail to open the lock if not validated by a specific time. The key could contain a keypad, fingerprint recognition system, or other personal identification or biometric system that would prevent lost or stolen keys being used by others. The key could count the number of locks opened or store an identifying number of the locks opened. It could also store the times and dates of opening. The lock could be of any type and may or may not require the use of mechanical action from the key (in addition the electromagnetic power provided by the key for actuation of the lock). Types include padlocks, door locks, locks integral to handles, window locks, gate locks. The lock could contain a power source to maintain an electronic clock or calendar such that the lock could record the times and dates of opening or closing.

Figure 3 shows a flow chart of one method of exchanging codes between the key and lock, carrying out validation and reprogramming the lock. After the key is connected to the lock the lock is powered up and begins a start-up sequence, at the end of which a code is transmitted to the key. This code may contain company information, the current lock code version, zone information,

and other information needed by the key. On receipt of this information the key responds with a code which my be derived from some or all of the information received from the lock or may be derived by some other pre-determined means, such as a pseudo-random number sequence, a time or date based system. When the lock receives this response it performs initial validation of the key. Invalid keys will be rejected and the lock will go into a timed sequence to prevent 'picking' of the lock. The length of time between retries may be controlled by the company and zone information, to prevent inadvertent use of the wrong key causing long time-outs. The current time-out state will be saved to a non-volatile store so that if the key is removed, thus removing the power, the time-out will be preserved. Thus on start-up the lock will carry on the time-out from where it was interrupted. Use of a key with the wrong initial response may cause this time-out period to be very long, a matter of hours or days so that picking the lock by trying random codes will be very time consuming.

Having performed the initial validation the lock will continue to transmit segments of the code and perform validation of responses received from the key until the key is validated. At this point the lock will transmit its current version code. If the key determines this to be out of date it will enter a programme sequence and reprogramme the lock. Once this is done the lock will open.

In the above arrangement the exchange of information is from the lock to the key with the key providing coded responses. Many combinations of data exchange

have been considered including lock to key, key to lock, part form lock to key and part from key to lock, initiated by the key or bey the lock, by transmitting one part by one element (lock or key) and responding with the next part from the other element, the encrypted responses described above or any other arrangement. There may be circumstances where no one key can open a particular lock but two or more keys must be applied in succession before the lock will open. As described above these keys may also need a validating parameter, such as a code entered on a key pad or a biometric parameter such as a finger print or retina scan. This would ensure that not only is the key present but the key holder is also present.

Figure 4 shows a block diagram of an application for the invention in a security system. Here it is supposed that an area to be secured is split into three zones, one inside another; this may represent a building within a perimeter fence, for example. Each zone is secured with a different lock. The programming means is used to programme three keys (however, there need not be the same number of keys as locks or zones). The first key (key part 1) is programmed to open lock part 2 and lock part 3 thus allowing access to zones 2 and 3. Key part 2 is only programmed to open lock part 1 and key part 3 opens all locks and is therefore a master key. Clearly the user of key part 1 can only access zones 2 and 3 if one of the other key holders has granted access to zone 1. As an example, suppose that zone 1 is the perimeter fence of an industrial unit, zone 2 is the building and zone 3 is the office within the building. Key part 2 is programmed for the groundsman and only allows access to the grounds, key part 1 allows office staff access during normal

12

hours when the perimeter gate is open and key part 3 allows the security staff access to all areas. Should any one of these key be lost, or if one is taken by an employee who leaves, the keys and locks can be reprogrammed to render the missing key ineffective.

Any number of zones, within the capability of the memory of one key part, could be configured and each key holder would only need one key. The zones could be arranged in any way, from completely separate to completely nested as in the above example but more typically would be a mixture of nested and separate zones.

CLAIMS

1   A programmable security lock which is programmed with a security code which controls the opening of a catch thereof, said lock comprising an electronic key part which is programmed with a security code which corresponds to that of a lock part, in which the key part is capable of opening the catch when it has been coupled to said lock part and when comparison means has confirmed agreement of the security code.

2   A lock as claimed in Claim 1, in which the lock part includes an electronic circuit having a security code memory and a catch release mechanism, and which is energised only when the electronic key part is coupled to said lock part.

3   A lock as claimed in Claim 2, in which the lock part electronic circuit further includes a security code checking circuit capable of returning a checking response to the electronic key part.

4   A lock as claimed in Claim 3, in which the electronic key part upon receiving a checking response from the lock part is arranged to send an acknowledgement signal to the lock part circuit.

5   A lock as claimed in Claim 3 or 4, in which the key part and the lock part electronic circuits are capable of exchanging a series of checking signals

14

to ensure correct validation of the security code.

6   A lock as claimed in any one of Claims 1 to 5, in which the electronic key
    part includes a memory capable of retaining the security code that has
    been programmed into the key, the said memory being capable of being
    programmed again to retain a new security code.

7   A lock as claimed in Claim 6, in which the electronic key part upon being
    coupled to the said lock part is capable of programming the said new
    security code into the lock part memory to replace the original security
    code thus ensuring that the new security code will control the catch
    opening.

8   A programmable security lock substantially as hereinbefore described with
    reference to any one of the accompanying drawings.

9   A programmable security lock system, comprising a security lock as claimed
    in any one of Claims 1 to 8 and programming means for changing a stored
    security code in the said key part.

10 A programmable security lock system, substantially as hereinbefore
    described.

CLAIMS

1. A programmable security lock which is programmed with a security code which controls the opening of a catch thereof, said lock comprising an electronic key part which is programmed with a security code which corresponds to that of a lock part, in which the key part is capable of opening the catch when it has been coupled to said lock part and when comparison means has confirmed agreement of the security code, in which the lock part includes an electronic circuit having a security code memory and a catch release mechanism, an electrical power supply for the lock being provided by the electronic key part only at a time when the key part is coupled to said lock part.

2. A lock as claimed in Claim 1, in which the lock part electronic circuit further includes a security code checking circuit capable of returning a checking response to the electronic key part.

3. A lock as claimed in Claim 1 or 2 in which the electronic key part upon receiving a checking response from the lock part is arranged to send an acknowledgement signal to the lock part circuit.

4. A lock as claimed in Claim 1,2 or 3, in which the key part and the lock part electronic circuits are capable of exchanging a series of checking signals to ensure correct validation of the security code.

5. A lock as claimed in any one of Claims 1 to 4, in which the electronic key part includes a memory capable of retaining the security code that has been programmed into the key, the said memory being capable of being programmed again to retain a new security code.

6. A lock as claimed in any one of Claims 1 to 5, in which the electronic key part includes two or more memories capable of

16

retaining a security code, the said security codes being capable of releasing the catch mechanisms of two or more differently coded lock parts.

7. A lock as claimed in any one of Claims 1 to 6, in which the electronic key part upon being couple to the said lock part is capable of programming the said new security code into the lock part memory to replace the original security code thus ensuring that the new security code will control the catch opening.

8. A programmable security lock substantially as hereinbefore described with reference to any one of the accompanying drawings.

9. A programmable security lock system, comprising a security lock as claimed in any one of Claims 1 to 8 and programming means for changing a stored security code in the said key part.

10.A programmable security lock system, comprising a security lock as claimed in any one of Claims 1 to 8, in which the system includes separate zones having individual locks protecting access to the different zones of the system, in which a particular key part has memory means arranged to allow access to one or more of the said zones.

11.A programmable security lock system, substantially as hereinbefore described.

Application No:	GB 9615898.5	Examiner:	A Angele
Claims searched:	All	Date of search:	18 October 1996

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

    UK Cl (Ed.O): E2A(ALV, AEE)

      Int Cl (Ed.6): E05B-049/00

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2260563 A	R TOMS	1,2 at least
X	GB 2259737 A	KILDL TECH. CORP.	1 at least
X	GB 2188762 A	P H BERTENSHAW	1 at least
X	WO86/01360 A	COMPUTERISED SECURITY SYST. (See especially para 2 p12; para 1 p16)	1,2 at least
X	WO86/00108 A1	LOWE & FLECHER (See especially para 4 p10)	1,2 at least
X	WO80/02711 A1	ID-SE-LECT BO THELIN	1 at least
X	WO80/00091 A1	R MOSCIATTI	1,2 at least
	See whole document unless otherwise indicated.		

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
		E	Patent document published on or after, but with priority date earlier
&	Member of the same patent family		than, the filing date of this application.